Discrete Mathematics 84 (1990) 71–85
North-Holland

ON SPLITTING SETS IN BLOCK DESIGNS AND FINDING ROOTS OF POLYNOMIALS

P.C. VAN OORSCHOT†, S.A. VANSTONE†‡
†*Department of Computer Science*
‡*Department of Combinatorics and Optimization*
University of Waterloo, Waterloo, Ontario, Canada

Received 28 September 1987

The general notion of t-splitting sets is introduced within the context of combinatorial block designs. A greatest lower bound on cardinality of such sets, and an upper bound on cardinality of the smallest such set in a given design are established. The abstraction of t-splitting sets is shown to provide a natural framework for the analysis of the problem of finding roots of polynomials over finite fields, and elementary concepts from design theory are applied to re-examine and extend some existing results in this area.

1. Introduction

We introduce the abstract notion of t-splitting sets within the context of combinatorial blocks designs, and provide general lower and upper bounds on their size. As an application, we use the framework of t-splitting sets to discuss the problem of finding roots of polynomials over finite fields. We note the formulation of an algorithm of Berlekamp, based on the intersection properties of specific hyperplanes of AG(n, q), from this framework. In greater detail, we consider the Berlekamp–Rabin probabilistic root-finding technique and its generalization to root-finding via a subgroup and its cosets. Using standard methods from design theory, new exact probabilities regarding this algorithm are established, and it is shown how the lower and upper bounds on the size of t-splitting sets can be used to generalize some bounds of Camion. Isolating roots of a polynomial being a special case of separating the root set into subsets of cardinality less than t, we extend the analysis of the Berlekamp–Rabin algorithm and determine the exact probability that a triple of roots is separated.

2. Fundamentals

For our purposes, a *block design* shall be an ordered pair (V, B) where V is a set of elements (called *points*) and B is a collection of subsets (called *blocks*) of V. A design is said to be *resolvable* if there exists a partition of the blocks into classes (*resolution classes*) such that each point of V is contained in exactly one

block of each class. Let D be a resolvable block design having v points, r resolution classes and at most n blocks per resolution class. Let $S = \{R_1, R_2, \ldots, R_r\}$ be the set of resolution classes of D. Let t be an integer, $1 < t < v$. We define a *t-splitting set* of D to be a set $S_t = \{R_{i_1}, R_{i_2}, \ldots, R_{i_s}\}$, $s \leq r$, such that each choice of a set of blocks $B_j \in R_{i_j}$, $1 \leq j \leq s$, satisfies the relation $|\bigcap_{j=1}^{s} B_j| < t$.

Less formally, a t-splitting set of D is a subset S_t of the set of resolution classes of D with the property that no t-subset of the point set of D is contained in a block of every resolution class in S_t. If some t-subset occurs in a block of every resolution class of D, then D has no t-splitting set. If all blocks in some resolution class R_i of D have cardinality at most $t-1$, then R_i is by itself a t-splitting set.

We are interested in finding t-splitting sets of small cardinality. Aside from independent mathematical interest, we see in Section 3 that efficient methods for finding t-splitting sets in special classes of designs would give efficient and deterministic methods for finding roots of and factoring polynomials over finite fields. Our discussion begins by establishing a lower bound on the size of such sets.

Theorem 1. *Let D be a resolvable design on v points with at most n blocks per resolution class. If a t-splitting set S_t of D has cardinality s, then $s \geq \log_n v - \log_n(t-1)$.*

Proof. Let V be the point set of D. Given s resolution classes of D there exists a subset $X \subseteq V$, with $|X| \geq v/n^s$, which is contained in a block of each of the s classes. This statement can be easily proven by induction on s. If $v/n^s > t-1$ then some t-subset of V is contained in a block of each of the s classes. Since S_t is t-splitting, we must have $v/n^s \leq t-1$ and the result follows. □

Let S_t be a t-splitting set for a resolvable design D. Denote the lower bound of Theorem 1 by $\sigma(v, n, t)$, so that $|S_t| \geq \sigma(v, n, t)$. If $|S_t| = \sigma(v, n, t)$ we call S_t a *perfect* t-splitting set, and if $|S_t| = \lceil \sigma(v, n, t) \rceil$ we call S_t a *quasi-perfect* t-splitting set. If S_t^* is a t-splitting set for D such that $|S_t^*| \leq |S_t|$ for all t-splitting sets S_t of D, then S_t^* is an *optimal* t-splitting set for D. We define $\nu(D, t)$ to be the cardinality of an optimal t-splitting set in D. It is clear that $\nu(D, t)$ is a non-increasing function of t. A *minimal* t-splitting set for D is a t-splitting set which does not properly contain a t-splitting set. A design D which possesses a perfect t-splitting set is called a perfect t-splitting design.

Due to the limited structure imposed on the design D thus far, it is a relatively simple task to construct designs on v points with at most n blocks per resolution class which have quasi-perfect t-splitting sets (and perfect t-splitting sets when the numbers allow). A more interesting (and useful) situation arises when we require D to have additional structure. A design D in which every l-subset of the point set is contained in precisely λ_l blocks of D is known as an *l-wise balanced* design

(of index λ_l). For example, if D is a resolvable balanced incomplete block design (BIBD) with parameters (v, k, λ), the pair-balance $\lambda_2 = \lambda$ implies that any $\lambda + 1$ resolution classes form a 2-splitting (pair-splitting) set, giving directly an upper bound $\nu(D, 2) \leqslant \lambda + 1$. With this in mind, we define an *l-wise bounded* design D (of index λ_l) to be a design D in which no l-subset of the point set occurs in more than λ_l blocks of D.

In the examples which follow, we make use of the following general construct. Using as point set a finite abelian group G, and given a partition $\hat{B} = \{B_1, \ldots, B_n\}$ of G (the subsets $B_i \subset G$ being commonly referred to as *base blocks*), the design $D = \mathrm{dev}_G(\hat{B})$, known as the *development* of $\hat{B}$ by G, consists of $|G|$ resolution classes, with each $g \in G$ defining a class $\hat{B} + g = \{b_1 + g, \ldots, B_n + g\}$, where $B_i + g = \{b + g : b \in B_i\}$. We denote the finite field with q elements F_q, and (with q being understood) let R and N denote the quadratic residues and nonresidues of F_q, respectively.

Example 1. Consider F_{11} with $R = \{1, 3, 4, 5, 9\}$ and $N = \{2, 6, 7, 8, 10\}$. With $G = F_{11}$, $\mathrm{dev}_G(R, N \cup \{0\})$ is a pairwise-balanced design of index $\lambda_2 = 5$ on 11 points. A quasi-perfect pair-splitting set is $S_2 = \{R_0, R_1, R_2, R_4\}$, where $R_i = \{R + i, N \cup \{0\} + i\}$.

Example 2. Consider F_{31} with

$$R = \{1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 26, 28\}$$

$$N = \{3, 6, 11, 12, 13, 15, 17, 21, 22, 23, 24, 26, 27, 29, 30\}.$$

Using $G = F_{31}$, $D = \mathrm{dev}_G(R, N \cup \{0\})$ is a pairwise-balanced design of index $\lambda_2 = 15$. Exhaustive search reveals that D contains no pair-splitting set of cardinality $\lceil \sigma(31, 2, 2) \rceil = 5$, and that $\nu(D, 2) = 6$. Many optimal pair-splitting sets exist, one being $S_2 = \{R_0, R_1, R_2, R_3, R_5, R_{28}\}$ (with R_i as in Example 1).

Example 3. For F_{31} with notation as in Example 2, it is well-known that $\mathrm{dev}_G(R, N)$ is a $(31, 15, 14)$-BIBD and easy to show that $D = \mathrm{dev}_G\{R \cup \{\infty\}, N \cup \{0\})$ is a $(32, 16, 15)$-BIBD. (Here ∞ is an indeterminate element with $a + \infty = \infty + a = \infty$.) It follows from Example 2 that D contains no perfect pair-splitting set.

Example 4. Consider $F = F_{2^n}$, generated by a root α of a primitive polynomial $f(x)$ of degree n over F_2. Let $B_0 = \{i : \mathrm{tr}(\alpha^i) = 0,\ \alpha^i \in F\}$, where $\mathrm{tr}(\beta) = \sum_{i=0}^{n-1} \beta^{2^i}$ and $0 = \alpha^\infty$, and let $B_1 = \{i : \mathrm{tr}(\alpha^i) = 1,\ \alpha^i \in F\}$. For $n = 5$ and $f(x) = x^5 + x^2 + 1$ we have

$$B_0 = \{1, 2, 4, 7, 8, 14, 15, 16, 19, 23, 25, 27, 28, 29, 30, \infty\}$$

$$B_1 = \{0, 3, 5, 6, 9, 10, 11, 12, 13, 17, 18, 20, 21, 22, 24, 26\}.$$

It is easy to verify that the set of resolution classes $S_2 = \{R_i : 0 \leq i \leq 4\}$, where $R_i = (B_0 + i, B_1 + i)$, with points (excepting ∞) treated as integers modulo 31, is a perfect pair-splitting set. Then by definition, a resolvable design on 2^5 points containing the resolution classes in S_2 as a subset of its resolution classes is a perfect pair-splitting design. It can be shown that the design with resolution classes R_i, $0 \leq i \leq 2^n - 2$ is a $(2^n, 2^{n-1}, 2^{n-1} - 1)$-BIBD isomorphic to the block design obtained from the points and hyperplanes of AG(n, 2).

We note that Example 4 illustrates a (32, 16, 15)-BIBD which possesses a perfect-pair-splitting set, while Example 3 illustrates a BIBD with the same parameters which does not.

An upper bound on the cardinality of an optimal t-splitting set for a design D with parameters v and r, which is t-wise bounded of index $\lambda_t < r$, can be established as follows. Let V be the point set of D. Construct a new design $\hat{D}$ from D with point set $\hat{V}$ being the classes of D, and having precisely one block for each t-subset of V. In $\hat{D}$, let the block corresponding to a given t-subset contain as points precisely those classes of D in which that t-subset occurs. Then each block of $\hat{D}$ contains at most λ_t points, and $\hat{D}$ is composed of $\binom{v}{t}$ blocks. Now the number of (not necessarily distinct) h-subsets from blocks of $\hat{D}$ is at most $\binom{\lambda_t}{h}\binom{v}{t}$, and the total number of distinct h-subsets of $\hat{V}$ is $\binom{r}{h}$. Now if $\binom{r}{h}$ exceeds $\binom{\lambda_t}{h}\binom{v}{t}$, then some h-subset of $\hat{V}$ does not appear as a subset of any block of $\hat{D}$, implying that the h classes of D corresponding to those h points of $\hat{V}$ contain no common t-subset, i.e. form a t-splitting set. Hence the smallest h satisfying

$$\binom{r}{h} > \binom{\lambda_t}{h}\binom{v}{t} \tag{1}$$

gives an upper bound on $v(D, t)$. We pursue an explicit bound from (1). As mentioned earlier, $h = \lambda_t + 1$ trivially satisfies (1) and gives an upper bound, but in general this bound is weak. Assume $h \leq \lambda_t$ satisfies (1). Let ρ (not necessarily integral) be defined by $\lambda_t / r = 1/\rho$. $1/\rho$ then gives an upper bound on the fraction of classes in D in which any t-subset occurs. With this, (1) becomes

$$\rho^h \frac{r(r-1)\cdots(r-(h-1))}{r(r-\rho)\cdots(r-(h-1)\rho)} > \binom{v}{t}$$

which is true for all h satisfying

$$\rho^h \geq \left(\frac{v}{t}\right).$$

Hence we have the following.

Theorem 2. *Let D be a resolvable design with parameters v and r, which is t-wise bounded of index $\lambda_t < r$, and let $\rho = r/\lambda_t$. Then $v(D, t) \leq \min\{\lambda_t + 1, \lceil \log_\rho \binom{v}{t} \rceil\}$.*

The smallest h satisfying (1) may give a slightly tighter bound than that of Theorem 2. This may be easily checked once the bound from Theorem 2 has been computed. Note that since $\binom{v}{t} \leq v^t/t!$, a slightly weaker but perhaps more informative bound is $\nu(D, t) \leq \lceil t \log_\rho n - \log_\rho(t!) \rceil$. The bound of Theorem 2 may also be obtained using the counting argument of Adleman [2, §IV]. Our proof uses a somewhat different counting technique, and is included for this reason.

The promising upper bound provides no efficient general technique for finding t-splitting sets of small size (i.e. $O(\log v)$). However, one particular family of designs is known for which perfect t-splitting sets can be easily found and efficiently represented (Section 3.1). For another family of designs useful for root-finding and polynomial factorization (Section 3.2), small t-splitting sets are known to exist, although no general method for efficiently finding such sets is known.

3. Polynomial representation of blocks and application to root-finding

In this section we consider a natural polynomial representation for block designs over finite fields, and discuss the relationship between t-splitting sets and polynomial factorization.

Let D be a resolvable block design with block set B and point set $V = F_q$. Let $\psi : B \to F_q[x]$ associate a unique polynomial with each block of D, with $\psi(B) = f_B(x)$ where $f_B(x) = \prod_{i=1}^{k} (x - v_i)$ for the block $B = \{v_i\}_{1 \leq i \leq k}$. Suppose $S_t = \{R_1, \ldots, R_s\}$ is a t-splitting set on point set V, with $R_i = \{B_{i1}, \ldots, B_{in_i}\}$. Then given a degree-$k$ polynomial $f(x) \in F_q[x]$ which splits into distinct linear factors in F_q, we may separate its k roots into subsets of cardinality at most $t - 1$, represented by polynomials of degree at most $t - 1$, by calling the procedure *t_split*$(f(x), 1)$, defined as follows.

t_split(f, i)
  if $\deg(f) = 0$ return$(\emptyset)$
  if $\deg(f) < t$ return(f)
  for j from 1 to $n_i - 1$
    $f_i := \gcd(f, f_{B_{ij}}(x))$
    $f := f/f_j$
  $f_{n_i} := f$
  return$\left(\bigcup_{j=1}^{n_i} t_split(f_j, i + 1)\right)$

t_split$(f(x), 1)$ returns a set of polynomials $\{f_i\}_{1 \leq i \leq l}$ such that $f(x) = \prod_{i=1}^{l} f_i$ and $\deg(f_i) < t$. The t-splitting set S_t and the value t are assumed global inputs.

The second argument specifies the next resolution class of S_t to be employed. The maximum recursion depth is s, the cardinality of S_t, and the algorithm is guaranteed to terminate by the time the last resolution class of S_t is consulted ($i \leq s$). In the ith resolution class of S_t, only the first $n_i - 1$ blocks need be referenced explicitly, the last being handled by exclusion.

For $t = 2$, *t_split*( ) as given above is a deterministic root-finding algorithm, given a pair-splitting set S_2. For $t = 3$, a triple-splitting (3-splitting) set S_3 is required, and provides a root-finding algorithm given a method for computing the roots of a quadratic which splits over F_q. For q odd, the quadratic formula over F_q, together with a method for computing square roots would suffice. For $q \equiv 3 (\text{mod } 4)$, square roots are immediate. For $q \equiv 1 (\text{mod } 4)$, see for example [1, 17, 15]. For q even, the roots of a quadratic can be easily computed (e.g. [12]).

In general, for $t \geq 2$ *t_split*( ) is of use as a root-finding algorithm given S_t and an efficient method for finding roots of polynomials of degree at most $t - 1$. Berlekamp discusses the applicability and use of the classical formulas for finding roots of cubics and quartics [4, §7].

Using the representation outlined above, a polynomial of degree k is required to represent a block of k points. Given no further information, we expect a polynomial with about k terms. In general, it would be costly to store the associated polynomials for all blocks of each resolution class in S_t. Hence information regarding the automorphism group of the design may be of use. Of particular interest are designs with automorphism groups which act transitively on the resolution classes.

Example 5. For F_{31}, the blocks R and $N \cup \{0\}$ have polynomial representations $f_R(x) = x^{15} - 1$ and $f_{N \cup \{0\}}(x) = (x^{15} + 1)x$. In $\text{dev}_{F_{31}}(R, N \cup \{0\})$, block $R + i$ has polynomial representation $(x - i)^{15} - 1$. Alternatively, for the same field consider the design obtained by developing the base blocks $B_0 \backslash \{\infty\}$ and B_1 of Example 4. Then $f_{B_0 \backslash \{\infty\}}(x) = (x^{10} - 1)(x^5 - 5)$ and $f_{B_1}(x) = (x^{10} - 5)(x^5 + 5)x$. (In general, for a Mersenne prime $p = 2^n - 1$, associating exponents in F_{2^n} with elements of F_p as in Example 4 leads to polynomials of degree $(p - 1)/2$ and $(p - 1)/2 + 1$ with at most $(p - 1)/2n + 1$ terms. This follows from the polynomial representation of the subgroup of order n of F_p^* and its cosets.) As mentioned in Section 3.1, in this latter design, any n successive resolution classes provide a quasi-perfect pair-splitting set.

3.1. *The use of the affine geometry*

The problem which remains is that of finding t-splitting sets S_t. One solution is provided by a root-finding technique of Berlekamp [4, §5] based on the trace function $\text{tr}: F_{p^m} \rightarrow F_p$ defined by $\text{tr}(\beta) = \sum_{i=0}^{m-1} \beta^{p^i}$. Given a polynomial $f(x)$ known to be the product of distinct linear factors in $F_q[x]$, $q = p^m$, and an element α which is the root of an irreducible polynomial of degree m over F_p, the mp

greatest common divisor operations $\gcd(f(x), \mathrm{tr}(\alpha^i x) - j)$, $0 \leq i \leq m-1$, $0 \leq j \leq p-1$, are guaranteed to separate every pair of roots of $f(x)$. In terms of splitting sets, the set of resolution classes $S = \{R_i\}_{0 \leq i \leq m-1}$, where $R_i = \{B_{ij}\}_{0 \leq j \leq p-1}$, with $\psi(B_{ij}) = \mathrm{tr}(\alpha^i x) - j$, is a perfect pair-splitting set. In fact, for $n = p$ and any t, this construction yields a quasi-perfect t-splitting set for point set F_{p^m}.

Zierler discusses the particular case of finding roots in F_{2^m} of polynomials in $F_2[x]$ of degree m [20]. Rabin notes a probabilistic variation of this technique for $p = 2$ (which generalizes to p odd) which does not require a root α as mentioned above [16, §5].

Related issues regarding t-splitting sets and the intersection properties of blocks of the underlying design, i.e. the points and hyperplanes of the affine geometry $\mathrm{AG}(n, p)$, are examined in [18].

3.2. *The use of subgroups and cosets*

The best known method for finding roots of polynomials over F_q, q odd, is the probabilistic technique based on the separation of quadratic residues and nonresidues [4, §7, 16, §2]. Given $f(x)$ as before, a random element $d \in F_q$ is chosen, and

$$\gcd(f(x), (x+d)^{(q-1)/2} - 1) \tag{2}$$

is computed. With probability about $\frac{1}{2}$, this operation separates any two distinct roots of $f(x)$. This algorithm can be viewed as a probabilistic version of *t_split*( ), with underlying design $\mathrm{dev}_{F_q}(R, N \cup \{0\})$. Rather than using the ith resolution class of a pair-splitting set at the ith stage, a block is randomly chosen from $\mathrm{dev}_{F_q}(R)$ to perform a trial gcd. As the base block of quadratic residues R has polynomial representation $x^{(q-1)/2} - 1$, and the translated block $R + d$ has polynomial representation $(x-d)^{(q-1)/2} - 1$, picking a random element $d \in F_q$ correspond to selecting a random block from $\mathrm{dev}_{F_4}(R)$, and the two algorithms are seen to be equivalent.

Of course, the Berlekamp–Rabin root-finding algorithm is a special case of the general idea of exploiting a multiplicative subgroup and its cosets [13, 9, 6]. Given any small divisor n of $q-1$, and a primitive nth root of unity ω, we can replace (2) with

$$\gcd(f(x), (x+d)^{(q-1)/n} - \omega^j), \quad 0 \leq j \leq n-1. \tag{3}$$

Each polynomial $x^{(q-1)/n} - \omega^j$, $0 \leq j \leq n-1$ has as root set the elements of one coset of the subgroup of index n of the multiplicative group of F_q. The corresponding design is now the development of a subgroup and its cosets (and to be precise, the base block $\{0\}$, corresponding to the polynomial x, included to complete the resolution classes). The analysis of this generalized root-finding algorithm is simplified by the following well-known result from design theory (e.g. [19, §7]).

Theorem A. *Let α be a generator for F_q, with $q-1=kn$, and let the multiplicative subgroup of index n be $C=\{\alpha^0, \alpha^n, \alpha^{2n}, \ldots, \alpha^{(k-1)n}\}$. Then* $\mathrm{dev}_{F_q}(C, \alpha C, \alpha^2 C, \ldots, \alpha^{n-1}C)$ *is a* $(q, k, k-1)$-BIBD.

It follows directly that for q odd, the development of the residues and nonresidues, dev(R, N), is a $(q, (q-1)/2, (q-3)/2$-BIBD. In Section 4, we use this structure to determine the exact probability of separating two roots via (2), and we extend the analysis to determine the exact probability that a triple of roots is separated via (2).

This general result can also be related to the general factorization problem. Camion [7, 8] discusses a factorization technique based on finding the primitive idempotents of the algebra $F_q[x]/(f(x))$. This can be seen as a deterministic version of the method of Cantor and Zassenhaus [9], with the determinism relying on the possession of Camion's "factoring subsets". These are (with minor discrepancy) equivalent to pair-splitting sets based on a subgroup and its cosets, i.e. our 2-splitting sets are in essence a generalization of factoring subsets. Thus a pair-splitting set from the design based on a subgroup and its cosets would provide an efficient deterministic general factorization algorithm, when incorporated in Camion's algorithm, as well as an efficient deterministic root-finding algorithm directly, via Berlekamp–Rabin.

The above theorem provides designs and λ_2 values for Theorem 2. In particular, we have $\lambda_2^{(2)}=(q-3)/2$ for q odd and the design based on the subgroup of index 2, and $\lambda_2^{(3)}=(q-4)/3$ for even and $q\equiv 1 (\mathrm{mod}\ 3)$ and the design based on the subgroup of index 3 and its cosets. This, together with (1), provides an easy alternate proof to Camion's bounds on the sizes of pair-splitting sets (compare $\lambda_2^{(2)}$, $\lambda_2^{(3)}$ to equations (12), (22) of [7, §5]). Indeed, the above theorem, together with Theorems 1 and 2, provide lower and upper bounds on the size of t-splitting sets for the family of designs obtained as the additive development of a multiplicative subgroup and its cosets.

As noted earlier, it is the algebraic structure of the underlying design, which permits efficient polynomial representation of blocks (i.e. cosets and hyperplanes in this and the previous subsection, respectively), together with the efficiency of the Euclidean algorithm, that is the key to the effective separation of roots of polynomials.

4. Some probabilities regarding root-finding using subgroups and cosets

For a polynomial $f(x)$ of degree m with distinct linear factors over F_q, Rabin [16] argued that the probability of (2) yielding a nontrivial factorization is at least $\frac{1}{2}$, and Ben-Or [3, §2] has proven that the probability of (2) resulting in a nontrivial factorization is at least $1-2^{1-m}+O(q^{-\frac{1}{2}})$. For the cases $m=2$ and $m=3$, we are able to complement these results by determining the exact probabilities.

We begin by reviewing some basic concepts. For each subset B_i of an abelian group G, denote the *list of differences* for B_i (with repeated elements allowed in a list) $\text{diff}(B_i) = (a - b : a, b \in B_i, a \neq b)$, and if $\hat{B} = (B_1, \ldots, B_n)$ is a family of subsets of G, the list of differences for $\hat{B}$ is $\text{diff}(\hat{B}) = \bigcup_{1 \leq i \leq n} \text{diff}(B_i)$, where a union over lists means list concatenation. For $|G| = v$, a (v, k, λ)-*difference family* is a family $\hat{B}$ of k-subsets of G such that each nonzero $g \in G$ occurs in $\text{diff}(\hat{B})$ exactly λ times. It is well-known that $\text{dev}_G(\hat{B})$ is a (v, k, λ)-BIBD if and only if $\hat{B}$ is a (v, k, λ)-difference family.

Suppose F_q has a multiplicative subgroup of index $n \geqslant 2$. Let the subgroup and its cosets be $C_0 = C$, $C_1 = \alpha C, \ldots, C_{n-1} = \alpha^{n-1} C$. We now determine the probability that a pair of roots $\{a, b\} \in F_q$ is separated via (3), assuming (for efficiency) that only $n - 1$ of the n cosets in a given resolution class (say all but C_{n-1}) are consulted, just as in (2), only the quadratic residues are used. Clearly, if one checks all n cosets, the probability that a random resolution class separates the pair is $1 - \lambda/q$, where $\lambda = (q - 1)/n - 1$ independent of the pair, since it follows from Theorem A that $\text{dev}(C_0, \ldots, C_{n-1}, \{0\})$ is pairwise-balanced of index $\lambda_2 = \lambda$. Thus we analyze the pair-balance of the design $\text{dev}(C_0, \ldots, C_{n-2}, C_{n-1} \cup \{0\})$.

Let $\hat{B} = (C_0, \ldots, C_{n-1})$, $D = \text{dev}(\hat{B})$, $\hat{B}_0 = (C_0, \ldots, C_{n-2}, C_{n-1} \cup \{0\})$, and $D_0 = \text{dev}(\hat{B}_0)$. By Theorem A, each nonzero element of F_q appears in $\text{diff}(\hat{B})$ precisely $\lambda = (q - 1)/n - 1$ times. Appending 0 to the base block C_{n-1} modifies the pair-balance λ of D by introducing the differences $0 - c$ and $c - 0$, $c \in C_{n-1}$, to $\text{diff}(\hat{B})$. Now the number of blocks in D_0 containing the pair $\{a, b\}$ is equal to the frequency of the difference $d = a - b$ in $\text{diff}(\hat{B})$. Hence the frequency of the pair $\{a, b\}$ in D_0 is $\lambda^{(a,b)} = \lambda + \delta_1 + \delta_2$, where $\delta_1 = 1$ if $a - b \in C_{n-1}$ and 0 otherwise, and $\delta_2 = 1$ if $a - b \in C_{n-1+j(\text{mod } n)}$ and 0 otherwise, where $-1 \in C_j$. Since there are q resolution classs in total, the probability that a random resolution class separates the pair $\{a, b\}$ is $1 - \lambda^{(a,b)}/q$.

Example 6. $\alpha = 2$ is a generator for F_{13}, and the subgroup of index $n = 4$ and its cosets are $C_0 = \{1, 3, 9\}$, $C_1 = \{2, 5, 6\}$, $C_2 = \{4, 10, 12\}$, $C_3 = \{7, 8, 11\}$. We have $\lambda = 2$, $j = 2$ and $\text{dev}(C_0, C_1, C_2, C_3 \cup \{0\})$ is a partially pairwise-balanced design with pair frequencies 2 and 3. The pair $\{1, 3\}$ has $\lambda^{(1,3)} = 3$, and $1 - 3 = 11 \in C_3$. The pair $\{1, 4\}$ has $\lambda^{(1,4)} = 2$, and $1 - 4 = 10 \in C_2$.

We single out two particular cases, beginning with $n = 2$. For $q \equiv 3 (\text{mod } 4)$, -1 is a quadratic non-residue, $j = 1$ and it follows that $D = \text{dev}_{F_q}(R, N \cup \{0\})$ is pairwise-balanced of index $\lambda_2 = (q - 1)/2$. For $q \equiv 1 (\text{mod } 4)$, $j = 0$ and hence D is partially pairwise-balanced, with pairs whose difference is a quadratic residue having pair-balance $(q - 3)/2$, and pairs with nonresidue difference having pair-balance $(q + 1)/2$. Hence we have the following corollary to Theorem A.

Corollary 1. *The probability that the pair of roots* $\{a, b\} \subset F_q$ *is separated by a random step of the Berlekamp–Rabin algorithm is exactly* p, *where*

(i) *for* $q \equiv 3 (\mathrm{mod}\ 4)$, $p = (q+1)/2q$;

(ii) *for* $q \equiv 1 (\mathrm{mod}\ 4)$, $p = (q+3)/2q$ *if* $a - b \in R$, *and* $p = (q-1)/2q$ *if* $a - b \in N$.

For subgroups of index 3 in fields of characteristic 2, the particular result is as follows.

Corollary 2. *For* F_q *with* $q = 2^{2m}$, *let* C_0 *be the subgroup of index* 3, *with cosets* C_1 *and* C_2, *and let* $\lambda = (q-4)/3$. *The frequency* $\lambda^{(a,b)}$ *of the pair* $\{a, b\}$ *in* $\mathrm{dev}_{F_{2^m}}(C_0, C_1, C_2 \cup \{0\})$ *is* λ *if* $a - b \in C_0$ *or* C_1, *and* $\lambda + 2$ *if* $a - b \in C_2$. *The probability that a random resolution class separates* $\{a, b\}$ *is* $1 - \lambda^{(a,b)}/q$.

We note that the analysis of Cantor and Zassenhaus for their general factorization algorithm [9, §3], when reduced to the particular case of root-finding, differs slightly in two ways. First, they use linear factors $ax + d$, whereas the original Berlekamp–Rabin algorithm uses only monic linear factors. Replacing the monic factor in (3) by the general linear factor has a balancing effect. For example for $n = 2$, this enlarges the underlying design, so that instead of sampling from among the classes of $\mathrm{dev}(R, N \cup \{0\})$, the sample space is (effectively) the union of the resolution classes from $\mathrm{dev}(R, N \cup \{0\})$ and $\mathrm{dev}(N, R \cup \{0\})$, so that the probability of separation is $p = (q+1)/2q$ for all pairs $\{a, b\}$, for both $q \equiv 1$ and $3 (\mathrm{mod}\ 4)$. Second, they determine the probability assuming two gcd's are computed for a resolution class, whereas as in the analyses of Rabin and Ben-Or, we assume only one gcd is computed. The analysis of [9] reduced to the case of two linear factors determines the probability of non-separation to be $(q-3)/2q$, as given directly by the pair-balance of the design $\mathrm{dev}(R, N, \{0\})$. For $q = 2^{2m}$, the corresponding probability from their analysis, which is associated with the design $\mathrm{dev}(C_0, C_1, C_2, \{0\})$ (which we know has pair balance $(q-4)/3$), is naturally $(q-4)/3q$.

We now extend the analysis for the standard Berlekamp–Rabin algorithm (i.e. using residues and nonresidues) to triples of roots, to determine the probability a triple $\{a, b, c\} \in F_q$ is separated into two proper subsets. We rely on the following result.

Lemma 1. *For* F_q *with* q *odd, let* $D = \mathrm{dev}(R, N \cup \{0\})$.

(i) *For* $q \equiv 3 (\mathrm{mod}\ 4)$, D *is threewise-balanced of index* $\lambda_3 = (q-3)/4$.

(ii) *For* $q \equiv 1 (\mathrm{mod}\ 4)$, D *is partially threewise-balanced. Each triple appears with frequency* $(q+3)/4$, $(q-1)/4$, $(q-5)/4$ *or* $(q-9)/4$.

Part (i) of Lemma 1 is well-known (e.g. [14]). To prove (ii), we first establish two smaller results.

Lemma 2. *For F_q with $q = 4m + 1$, the number of common points between any two blocks from different parallel classes of $D = \mathrm{dev}_{F_q}(R, N)$ is m or $m - 1$.*

Proof. Label the blocks in the first class of D B_1 and B_2, and in the ith class, B_{2i-1} and B_{2i}, $3 \leqslant i \leqslant q$. Let $x_i = |B_1 \cap B_i|$, $3 \leqslant i \leqslant q$. Now B_q intersects each block B_i, $i \geqslant 3$ in m or $m - 1$ points if and only if

$$\sum_{i=3}^{2q} (x_i - m)(x_i - [m-1]) = 0.$$

Expanding the left side, we get

$$L = \sum x_i^2 - (2m-1) \sum x_i + \sum m(m-1).$$

Now D is a $(v, k, \lambda) = (q, (q-1)/2, (q-3)/2)$-BIBD, and counting the appearance of pairs of points from B_1 over blocks B_3 through B_{2q} yields $\sum_{i=3}^{2q} \binom{x_i}{2} = (\lambda - 1)\binom{k}{2}$, giving $\sum x_i^2 = (\sum x_i) + 2(\lambda - 1)\binom{k}{2}$ and

$$L = 2(\lambda - 1)\binom{k}{2} - (2m-2) \sum x_i + \sum m(m-1).$$

Now counting the appearances of the k points of B_1 over the rest of the design gives the relation $\sum x_i = (r-1)k$ (with $r = q - 1$ the replication value of D). With this the expression simplifies to $L = 0$, and block B_1 intersects each block B_i, $i \geqslant 3$, in m or $m - 1$ points. Since no special properties of B_1 were used, the same holds true for B_2, and the result follows. □

Lemma 3. *In* diff(R) *for F_q with $q \equiv 1 (\mathrm{mod}\, 4)$, every residue occurs with frequency $(q-5)/4$, and every nonresidue occurs with frequency $(q-1)/4$.*

Proof. We first establish that in diff(R) for F_q with $q = 4m + 1$,

(i) all residues occur with the same frequency, and

(ii) all nonresidues occur with the same frequency.

To prove (i), suppose there exists points $a, b \in R$ such that $a - b = d$ where $d \in R$. (If not, no residue appears as a difference.) Then since $d \in R$, $d^{-1} \in R$ and $d^{-1}d = 1 = d^{-1}(a - b)$. Hence $d^{-1}a - d^{-1}b = 1$ with $d^{-1}a$, $d^{-1}b \in R$, i.e. $1 \in$ diff(R). Now choose any $r \in R$. Then $r(d^{-1}a - d^{-1}b) = rd^{-1}a - rd^{-1}b = r$ with $rd^{-1}a$, $rd^{-1}b \in R$. Hence each residue r appears in diff(R) at least as often as 1. Similarly, it can be argued that 1 appears in diff(R) at least as often as each other residue difference r. The proof of (ii) is similar.

Now let χ be the quadratic character defined on F_q by $\chi(0) = 0$, $\chi(x) = 1$ if

$x \in R$ and $\chi(x) = -1$ if $x \in N$. Consider any $a \in R$, and the block $N - a$. Note $|N - a| = 2m$. By Lemma 2, $|N - a \cap R| = m$ or $m - 1$, and $|N - a \cap N| = m$ or $m - 1$. Since $a \in R$ implies $0 \notin N - a$, we have $|N - a \cap R| = m$ and $|N - a \cap N| = m$, and hence $\sum_{y \in N} \chi(y - a) = 0$. We now make use of the identity

$$\sum_{x \in F_q} \chi(x)\chi(x - a) = -1 \quad \text{for any } a \in F_q,\ a \neq 0 \tag{4}$$

from elementary number theory (e.g. [5, §9.12]). It follows from (4) that $\sum_{x \in R} \chi(x)\chi(x - a) + \sum_{y \in N} \chi(y)\chi(y - a) = -1$, and hence $\sum_{x \in R} \chi(x - a) = -1$, i.e. $R - a$ contains one more nonresidue than residue. Since this is independent of the residue a selected, we have $\sum_{a \in R} \sum_{x \in R} \chi(x - a) = -(q - 1)/2$, and diff$(R)$ contains $(q - 1)/2$ more nonresidues than residues. The result now follows from (i) and (ii). □

Remark. In diff(N) for $q = 4m + 1$, residues occur with frequency $(q - 1)/4$ and nonresidues with frequency $(q - 5)/4$. This follows from Lemma 3 and Theorem A.

Proof of Lemma 1(ii). For $q = 4m + 1$, consider $D = \text{dev}(R, N \cup \{0\})$, and let $D_R = \text{dev}(R)$. We count the frequency of a fixed triple $\{a, b, c\} \subset F_q$ among the blocks of D by first counting the frequency among blocks of D_R. Among the blocks of D_R, let s be the number of blocks containing none of a, b, c, let t be the number containing all three, let λ_{ab} be the frequency of the pair $\{a, b\}$, and similarly define λ_{ac} and λ_{bc}. We know that each individual point has replication value $(q - 1)/2$ in D_R. Now by the inclusion-exclusion principle,

$$s = q - 3\frac{(q-1)}{2} + (\lambda_{ab} + \lambda_{ac} + \lambda_{bc}) - t = \frac{(-q+3)}{2} + (\lambda_{ab} + \lambda_{ac} + \lambda_{bc}) - t.$$

Now for each of the t blocks in D_R containing the triple (and for no other blocks), the complementary block in D contains none of the three. Hence in D, the number of blocks containing none of the three points is $s + t = \eta(a, b, c)$ where

$$\eta(a, b, c) = (-2m + 1) + \lambda(a, b, c) \quad \text{with } \lambda(a, b, c) = (\lambda_{ab} + \lambda_{ac} + \lambda_{bc}).$$

Note that $\eta(a, b, c)$ is also the number of blocks in D containing all three points. The values λ_{ab}, λ_{bc}, λ_{ac} can be determined as follows. The pair $\{a, b\}$ appears exactly once for each occurrence of the difference $d = a - b$ in diff(R). The number of times this difference appears is a function only of whether d is a residue (in which case it appears $m - 1$ times, by Lemma 3), or a nonresidue (in which case it appears m times), and is otherwise independent of a and b. Similarly for the pairs $\{a, b\}$, $\{b, c\}$. The four values $\eta(a, b, c)$ takes, corresponding to four values $\lambda(a, b, c)$ can take, are summarized as follows.

# of nonresidue difference	# of residue differences
3	0
2	1
1	2
0	3

$\lambda(a, b, c)$	$\eta(a, b, c)$
$3m$	$m+1$
$3m-1$	m
$3m-2$	$m-1$
$3m-3$	$m-2$

Hence the only possible frequencies of a triple are $m+1$, m, $m-1$ and $m-2$. □

Example 7. Consider $\mathrm{dev}(R, N \cup \{0\})$ for F_{13}. The four frequencies of triples are exhibited by the triples $\{2, 5, 6\}$, $\{2, 5, 3\}$, $\{2, 5, 7\}$ and $\{2, 4, 9\}$, which occur 1, 2, 3 and 4 times respectively.

Lemma 1 now yield the following result directly.

Theorem 3. *The probability that the triple of roots $\{a, b, c\} \subset F_q$ is separated into two proper subsets by a random step of the Berlekamp–Rabin algorithm is p, where*

(i) *for $q \equiv 3 (\mathrm{mod}\ 4)$, $p = (3q+3)/4q$;*

(ii) *for $q \equiv 1 (\mathrm{mod}\ 4)$, depending on the number of residues and nonresidues among the differences $a-b$, $a-c$ and $b-c$ (as in the table in the proof of Lemma* 1(ii), *p has value $(3q-3)/4q$, $(3q+1)/4q$, $(3q+5)/4q$, or $(3q+9)/4q$.*

Remark. Lemma 1 and the remarks immediately preceding Corollary 1 provide values λ_3 and λ_2 that can be used in (1) to get an upper bound on the size of pair-splitting sets and triple-splitting sets, respectively, for the design $D = \mathrm{dev}(R, N \cup \{0\})$. The bounds $\nu(D, 2) < 2 \log_{2q}$ and $\nu(D, 3) < \frac{3}{2} \log_2 q$ can be established. The remarks preceding Example 6 allow the establishment of an upper bound on the size of pair-splitting sets for $D = \mathrm{dev}(C_0, C_1, C_2 \cup \{0\})$ for $q = 2^{2m}$. We note that the values $\lambda_2^{(2)}$ and $\lambda_2^{(3)}$ given earlier actually apply to the designs $\mathrm{dev}(R, N, \{0\})$ and $\mathrm{dev}(C_0, C_1, C_2, \{0\})$.

5. Comments and conclusion

While it is hoped that the concept of t-splitting set finds application in other contexts, and opens up some interesting problems for combinatorialists, we

believe it provides a natural view of the general root-finding problem and a useful and somewhat unifying perspective for existing results. The exact analysis of the original Berlekamp–Rabin algorithm, and the generalization of Camion's bounds for pair-splitting sets can be seen to follow directly from elementary design theory. We cite [10] and [11] as other recent applications of the theory of block designs to the design and analysis of algorithms.

The consideration of triple-splitting sets follows naturally as a special case of t-spitting sets, and would appear to be of interest to those in the area of polynomial factorization. We note that if a single root of a polynomial $f(x) \in F_q[x]$ of odd degree is required, then a triple-splitting set suffices, and if $f(x)$ has even degree, a triple-splitting set suffices unless $q \equiv 1 (\mathrm{mod}\ 4)$, in which case an algorithm for computing square roots in the field is also required.

It remains an open problem as to whether or not pair-splitting sets in designs based on a subgroup and its cosets can be efficiently found. The problem of finding other families of designs which support (small) splitting sets which can be efficiently represented is perhaps also worth pursuing.

References

[1] L. Adleman, K. Manders and G. Miller, On taking roots in finite fields, Proc. IEEE 18th IEEE Symp. Foundations Comp. Sci. (1977) 175–178.

[2] L. Adleman, Two theorems on random polynomial time, Proc. 19th IEEE Symp. Foundations Comp. Sci. (1978) 75–83.

[3] M. Ben-Or, Probabilistic algorithms in finite fields, Proc. 22nd IEEE Symp. Foundations Comp. Sci. (1981) 394–398.

[4] E.R. Berlekamp, Factoring polynomials over large finite fields, Math. Comp. 24 (1970) 713–735.

[5] T. Beth, D. Jungnickel and H. Lenz, Design Theory (Bibliographisches Institut, Zurich, 1985).

[6] P. Camion, Un algorithme de construction des idempotents primitifs d'ideaux d'algèbres sur F_q, Annals Discrete Math. 12 (1982) 55–63.

[7] P. Camion, A deterministic algorithm for factorizing polynomials of $F_q[x]$, Annals Discrete Math. 17 (1983) 149–157.

[8] P.F. Camion, Improving an algorithm for factoring polynomials over a finite field and constructing large irreducible polynomials, IEEE Trans. Inform. Theory IT-29 (1983) 378–385.

[9] D.G. Cantor and H. Zassenhaus, A new algorithm for factoring polynomials over finite fields, Math. Comp. 36 (1981) 587–592.

[10] R.M. Karp and A. Wigderson, A fast parallel algorithm for the maximal independent set problem, J. ACM 32 (1985) 762–773.

[11] T.V. Lakshman and A.K. Agrawala, Efficient decentralized consensus protocols, IEEE Trans. Software Engrg. SE-12 (1986) 600–607.

[12] R.J. McEliece, Finite Fields for Computer Scientists and Engineers (Kluwer Academic Publishers, 1987).

[13] R.T. Moenck, On the efficiency of algorithms for polynomial factoring, Math. Comp. 31 (1977) 235–520.

[14] R.C. Mullin, A note on self-complementary designs, Proc. 5th Southeastern Conf. on Combinatorics, Graph Theory and Computing (1974) 591–598.

[15] R.C. Peralta, A simple and fast probabilistic algorithm for computing square roots modulo a prime number, IEEE Trans. Inform. Theory IT-32 (1986) 846–847.

[16] M.O. Rabin, Probabilistic algorithms in finite fields, SIAM J. Comput. 9 (1980) 273–280.
[17] R. Schoof, Elliptic curves over finite fields and the computation of square roots mod p, Math. Comp. 44 (1985) 483–494.
[18] P.C. van Oorschot and S.A. Vanstone, A geometric approach to root-finding in GF(q^n), IEEE Trans. Inform. Theory IT-35 (1989) 444–453.
[19] R.M. Wilson, Cyclotomy and difference families in elementary abelian groups, J. Number Theory 4 (1972) 17–47.
[20] N. Zierler, A conversion algorithm for logarithms on GF(2^n), J. Pure and Appl. Algebra 4 (1974) 353–356.
[21] P.C. van Oorschot, Combinatorial and computational issues related to finding roots of polynomials over finite folds, PhD. Thesis, University of Waterloo, 1988.